mgr Paweł Soja
Uniwersytet Jagielloński
pawelsoja92@gmail.com

CYBERBEZPIECZEŃSTWO JAPONII W XXI W.

JAPAN'S CYBERSECURITY IN THE 21ST CENTURY

Streszczenie: Japonia od dziesięcioleci uchodzi za technologicznego lidera oraz kolebkę największych na świecie przedsiębiorstw branży IT. Pomimo wielu osiągnięć na tym polu, kraj jeszcze do niedawna pozostawał w znacznym stopniu nieprzygotowany na wyzwania, jakie niesie ze sobą wzrost zjawiska cyberprzestępczości. Brak regulacji prawnych, instytucji zwalczających zagrożenia pochodzące z sieci oraz niedobór wyspecjalizowanych kadr zdolnych ochronić zarówno sektor państwowy, jak i prywatny trapił kolejne gabinety rządowe. Przygotowania do zbliżających się Igrzysk Olimpijskich w Tokio w 2020 r. częściowo zmieniły ten stan rzeczy, a ostatnie lata pokazują wzmożoną aktywność władz w niwelowaniu skutków zapóźnienia w polityce cybernetycznej. Celem poniższego artykułu jest przedstawienie dzisiejszego poziomu cyberbezpieczeństwa Japonii z uwzględnieniem największych zagrożeń, sposobów ich rozwiazywania w wymiarze lokalnym i międzynarodowym oraz wyzwań, jakie stoją przed państwem w najbliższych latach.

Słowa kluczowe: cyberbezpieczeństwo, Japonia, polityka cybernetyczna, hacking, zagrożenia cybernetyczne

Summary: For decades, Japan has been widely recognized as a technological leader and the cradle of the biggest IT companies on the international market. Despite many achievements, the country was until recently unprepared for new challenges related to the emergence of cybercrime and digital threats. The absence of law regulations and institutions combating cyber risks as well as the shortage of professionals who are able to protect public and private sectors posed a real nuisance for any government. Preparations for the forthcoming Winter Olympic Games in Tokyo 2020 have partially changed this state of things and recent years have shown an increased activity and improvements in cyber policy. The aim of this paper is to render today's level of Japanese cybersecurity with a special attention paid to the biggest IT threats, national and international ways of resolving those issues and the most serious challenges in the near future.

Keywords: cyber policy, cybersecurity, cybersecurity risks, hacking, Japan

Wstęp

Świat w coraz większym stopniu uzależnia się od przepływu i dostępu do informacji, a w przypadku wielu wysoko rozwiniętych społeczeństw czynności podejmowane przy wykorzystaniu narzędzi wirtualnej rzeczywistości zaczynają wyznaczać dominujący aspekt ich codziennej aktywności. Efekt cybernetyzacji życia dotyka w równej mierze użytkowników prywatnych, jak przedsiębiorców czy instytucje rządowe. Tym

samym globalny rynek szeroko pojętych usług technologii informacyjnej (IT) cechuje dynamiczny rozwój, w znacznym stopniu niezależny od dominujących trendów gospodarczych. Drzemiący w nim potencjał jest trudny do precyzyjnego oszacowania, jednak w przybliżeniu wartość sektora może osiągnąć nawet 23 bln dolarów w 2025 r. (Pawlak, Barmpaliou, 2017). Jedynie ułamek tej kwoty, tj. ok. 170 mld dolarów, ma wynieść udział usług związanych z cyberbezpieczeństwem (Morgan, 2015). Ten fakt nie umknął uwadze środowiskom przestępczym, których rozwój następuje symultanicznie wraz z dalszą ekspansją branży, o czym świadczy fakt, że dzisiaj coraz więcej osób wykorzystuje *hacking*[1] jako źródło oraz metodę zarabiania pieniędzy. Szacowana wielkość strat poczynionych przez cyberkryminalistów przewyższyła już wartość światowego rynku handlu narkotykami i wynosi ok. 388 mld dolarów w skali roku (Wasilewski, 2016).

Jeszcze pod koniec XX wieku pojęcie cyberataku powszechnie kojarzyło się z postępowaniem obliczonym na wywołanie efektu szoku i zainteresowania osobą sprawcy. Główną motywacją często stawała się chęć udowodnienia wyższości na polu biegłości w korzystaniu z oprogramowania i łamania systemów szyfrujących dane. Obecnie przyjmuje się dużą szerszą typologię związaną zarówno ze sposobami, jak i motywacją przeprowadzania nielegalnych operacji w Internecie. Wyróżnia się ataki ukierunkowane na wyrządzenie fizycznych szkód, czerpanie korzyści finansowych za pomocą giełdy bądź infrastruktury bankowej, szkody natury psychologicznej poczynione ofiarom napaści, a także zniszczenia obejmujące tkankę samej sieci, które są trudne do wychwycenia dla osób bez specjalistycznej wiedzy (Tsuchiya, 2011b). Elektroniczne szpiegostwo i działania dywersyfikacyjne godzące w tzw. infrastrukturę krytyczną zaczynają jednocześnie przeważać wśród pozamilitarnych sposobów prowadzenia zawoalowanych wojen pomiędzy państwami. Szczególnie jawnym przykładem takich praktyk pozostaje wroga polityka Korei Północnej wobec jej południowego sąsiada. Sytuacja na Półwyspie Koreańskim pośrednio determinuje zachowanie Japonii, innej wysoko rozwiniętej gospodarki Azji Wschodniej, która po latach zaniedbań dopiero wkracza na ścieżkę pełnej modernizacji w zakresie instytucjonalno-prawnego mierzenia się z zagrożeniami płynącymi z cyberprzestrzeni. Dla rządu i obywateli jest to swoisty wyścig z czasem, którego finisz wyznacza data organizacji letnich Igrzysk Olimpijskich w Tokio w 2020 r.

Japonia na celowniku hakerów

Japonia od wielu lat uchodzi za jednego z globalnych liderów sektora IT, pozostając niezmiennie największym rynkiem produktów informatycznych i telekomunikacyjnych na świecie oraz kolebką przełomowych branżowych rozwiązań na czele z wprowadzeniem płatności mobilnych czy dostępem do usług internetowych przy wykorzystaniu telefonii komórkowej. Według zestawień zgromadzonych w *The Global Information Technology Report* za 2016 r. w Japonii ponad 97% populacji posiada dostęp do sieci, a technologie informatyczno-komunikacyjne w żadnym innym miejscu na Ziemi nie

[1] W ujęciu prezentowanym przez Interpol *hacking* to przestępczość skierowana przeciwko systemom komputerowym przy wykorzystaniu rozmaitych narzędzi cybernetycznych i technik włamań.

odgrywają tak znaczącej roli w przypadku nawiązywania kontaktów biznesowych czy utrzymywania relacji z klientami. Powiązania lokalnej gospodarki z usługami IT nie idą jednak w parze z zapewnieniem jej podmiotom optymalnego poziomu bezpieczeństwa i ochrony przed przestępczością cybernetyczną. Ten sam raport plasuje Japonię dopiero na 27. miejscu pod względem rozwoju prawodawstwa odnoszącego się do przemysłu wysokich technologii i ledwie mieści się w czołowej dwudziestce państw o największej liczbie zaufanych serwerów internetowych w przeliczeniu na milion mieszkańców. W tym ujęciu japońskie zasoby pozostają trzykrotnie mniejsze niż potencjał Islandii czy Szwajcarii[2]. Należy przy tym zauważyć, że są to osiągnięcia zdecydowanie wybijające się ponad globalną średnią, lecz z uwagi na rosnącą digitalizację sfery politycznej i gospodarczej Japonia potrzebuje zdecydowanie mocniejszych środków prewencji.

Przedstawione statystyki znajdują swoje odzwierciedlenie w praktyce. Japonia stała się w ostatnim piętnastoleciu jednym z ulubionych punktów inwazji hakerów, a za moment przesilenia można uznać lata 2003–2005, kiedy wystąpił nagły wzrost liczby popełnianych cyberprzestępstw rzędu 65% (Thomas, 2009). Doszło wtedy m.in. do paraliżującego pracę ponad 400 tys. prywatnych komputerów zakażenia z rodzaju DDoS (*distributed denial of service*), które poprzez zaraźliwe boty i trojany[3] doprowadziło do blokady wywołanej zajęciem wszystkich wolnych zasobów w rodzaju pamięci sprzętu bądź pasma sieciowego. Łącznie w 2005 r. wykryto ponad 310 mln prób przejęcia kontroli nad komputerami zarejestrowanymi w Japonii (Gady, 2015b), a dekadę po tych wydarzeniach liczba ataków wyniosła w 2014 r. już ponad 25 mld. Oznacza to, że co sekundę przeprowadzanych jest ich niemal tysiąc, ale ze względu na fakt, że odnotowana aktywność pochodzi zazwyczaj z oficjalnych raportów policji, trzeba mieć świadomość istnienia dużego odsetka niewykrytych bądź też niezgłoszonych przypadków łamania prawa (Nippon Telegraph and Telephone, 2015).

Jak przekonuje sprawozdanie przygotowane przez firmę Trend Micro z siedzibą w Tokio, Japonia wykazuje największą podatność na wyciek informacji bankowych spośród wszystkich państw poddanych ewaluacji (Braue, 2014). Dalsze analizy uświadamiają, że sektor bankowy traci rocznie wirtualnymi kanałami ekwiwalent rzędu 110 mln dolarów, co odpowiada mniej więcej 0,02% tamtejszego budżetu (*Center for Strategic and International Studies* [CSIS], 2014). Nie jest to w regionie Azji Wschodniej i Południowo-Wschodniej wskaźnik rekordowy, lecz cyberbezpieczeństwu nadal przypisuje się miano japońskiej pięty Achillesowej, ponieważ obok Korei Południowej i Singapuru lokalna gospodarka zaliczana jest do grupy najbardziej podatnych na ataki cybernetyczne na całym kontynencie. Przeprowadzone na tym gruncie badania wykazały jej ponad dziewięciokrotnie wyższą wrażliwość niż wynosi średnia światowa (Deloitte, 2016). Istnienie w cieniu ciągłego zagrożenia nie przeszkadza Japonii w utrzymywaniu pozycji czołowego prekursora technologii informatycznych. Kraj tradycyjnie pozostaje

[2] Zob.: World Economic Forum, *The Global Information Technology Report 2016: Innovating in the Digital Economy*.

[3] Trojan (koń trojański) – potoczne określenie oprogramowania, które podszywa się pod rozmaite aplikacje, wprowadzając do systemu użytkownika ukryte i niepożądane funkcje.

w gronie trzech największych rynków IT na świecie, a całkowita wartość sektora cyberbezpieczeństwa została oszacowana w 2014 r. na kwotę 2,6 mld dolarów, przy czym perspektywy wzrostu każą przypuszczać, że do końca 2018 r. osiągnie on poziom przekraczający kwotę 3 mld dolarów (Department of Commerce, 2016b).

Korzystając z coraz bardziej wymyślnych środków przechwytywania informacji, takich jak *spoofing* (podszywanie się pod cudze adresy IP), *buffer overlow* (przeładowanie danymi) czy *ping of death* (zakłócenie responsywności serwera), hakerzy naruszają już nie tylko dobra cywilne, lecz podejmują także próby ugodzenia w tzw. infrastrukturę krytyczną. Pod tym pojęciem kryje się zespół podstawowych zasobów koniecznych dla prawidłowego funkcjonowania gospodarki i społeczeństwa, w tym instalacje łączności, transportu, ochrony zdrowia czy zaopatrzenia w żywność bądź energię. W przypadku państwa polegającego w tak dużym stopniu na nowoczesnych technologiach, gdzie wyżej wymienione obszary są sprężone z elektronicznymi systemami zarządzania i sterowania, widmo katastrofy obejmującej zakłócenia w ruchu lotniczym czy utratę kontroli nad przepływem wody przez tamy i zbiorniki wodne powinno być wystarczającym bodźcem do zwiększania zdolności kompleksowego reagowania. W niedalekiej przeszłości dochodziło na tym polu do stosunkowo niegroźnych – ze względu na wykorzystanie nieskomplikowanych algorytmów – ataków ze strony niezidentyfikowanych sprawców, m.in. w ramach przedsięwzięcia *Operation Dust Storm*. Ofiarą napaści padli usługodawcy związani z przemysłem wydobywczym, transportowym oraz sektorem energetycznym (Cyber Defence Magazine, 2015). W 2014 r. Ministerstwo Spraw Wewnętrznych poinformowało, że liczba ataków na obiekty infrastruktury krytycznej wyniosła 12,8 mld przypadków, co równa się liczbie około połowy wszystkich odnotowanych w kraju cyberprzestępstw (Japan Times, 2014).

W 2011 r. przedsiębiorstwo Mitsubishi Heavy Industries (MHI), które jest oficjalnie zakontraktowanym dostawcą broni i sprzętu wojskowego dla japońskiego rządu, doznało szkód wskutek ataku typu APT (*advanced persistent threats*) wykorzystującego zarażone złośliwym oprogramowaniem wiadomości mailowe. Nieostrożna weryfikacja przychodzących na konta pracownicze e-maili spowodowała zakażenie ponad osiemdziesięciu komputerów i odpowiadających połowie tej liczby serwerów (Tsuchiya, 2015). Perspektywa wycieku informacji dotyczących tajnych projektów obejmujących produkcję rakiet dalekiego zasięgu, łodzi podwodnych czy instalacji nuklearnych wzbudziła poważne zaniepokojenie wśród obserwatorów. Ze względu na ścisłą kooperację w wymiarze bezpieczeństwa, jaka od przeszło pół wieku rozwija się pomiędzy Japonią i Stanami Zjednoczonymi, oraz na fakt, że duża część technologii pochodzi bezpośrednio od amerykańskich dostawców, afera w siedzibie MHI stanowiła realne zagrożenie dla stabilności relacji obu państw. W wydanym kilka dni po zajściu oświadczeniu przedstawiciele zbrojeniowego giganta zaprzeczyli pogłoskom o dostaniu się w niepowołane ręce najbardziej newralgicznych danych, niemniej było to pierwsze tego rodzaju wydarzenie w Japonii (Lennon, 2011).

Kilka tygodni po zawirowaniach wokół MHI miał miejsce kolejny incydent związany z wyciekiem poufnych danych członków Diet, czyli japońskiego parlamentu. Prywatne wiadomości i dokumenty ponad 480 posłów zostały wykradzione i częściowo upu-

blicznione. Podobne zdarzenia występowały przez pozostałą część roku, dotykając tym razem pracowników Ministerstwa Rolnictwa, Leśnictwa i Rybołówstwa, Ministerstwa Spraw Zagranicznych oraz placówek japońskich ambasad i konsulatów ulokowanych na różnych kontynentach, co według opinii ekspertów potwierdzało obiegowe opinie o zaangażowaniu w proceder strony chińskiej. Czarna seria miała w ten sposób zbiec się z okrągłą rocznicą napaści Japonii na Chiny w 1931 r. (Ventre, 2012). Nieszczelność japońskich archiwów położyła się również cieniem na negocjacjach dotyczących wdrożenia Partnerstwa Transpacyficznego w 2013 r., a w maju dwa lata później krajem wstrząsnęła afera złamania zabezpieczeń narodowego serwisu ubezpieczeń społecznych i emerytur. Ponad 1,25 mln elektronicznych profili zarejestrowanych w nim użytkowników wydostało się na zewnątrz, prowokując szeroką debatę nad koniecznością rozwinięcia nowych mechanizmów prewencji (Reuters, 2015). Kradzieże akt personalnych są szczególnie istotne z psychologicznego punktu widzenia i budzą największe emocje wśród zwykłych obywateli. W Japonii skala tego zjawiska jest wciąż wyższa niż w większości innych krajów. W 2016 r. pokrzywdzeni w ten sposób ludzie stanowili grupę 12,6 mln osób, co implikuje, że jeden na dziesięciu obywateli padł ofiarą cyberprzestępczości (Japan Times, 2017).

Przeciwdziałanie i zarządzanie cyberbezpieczeństwem

W zakresie regulacji sektorowych Japonia przez wiele lat pozostawała w tyle, nie posiadając legislatury zorientowanej na otaczające ją wyzwania. Ciężko jest przy tym przypisać winę za te opóźnienia jednemu konkretnemu czynnikowi. Jeszcze na początku XXI wieku stosunkowo niewielu ludzi posiadało w Japonii dostęp do komputera (ok. 20%), a jeszcze mniej korzystało z szybkiego łącza online (Ventre, 2012). Mógł to być niewątpliwie czynnik hamujący postęp, podobnie jak ugruntowana przez wieki izolacjonistyczna mentalność i wrażenie nietykalności wobec negatywnych aspektów korzystania z zasobów wirtualnego świata. Wydawana przez Ministerstwo Obrony Japonii Biała Księga aż do 2010 r. nie zawierała żadnych śladów świadczących o znajomości terminu *cyberbezpieczeństwo* przez tamtejsze elity, podobnie jak puste w treści pozostawały wytyczne składające się na narodowe wytyczne dotyczące obronności (Kallender, Hughes, 2017). Biorąc pod uwagę technologiczną biegłość mieszkańców państwa oraz ich przewodnią rolę w branży IT, paradoks stanowiła sytuacja, w której do połowy 2010 r. w kodeksie karnym nie było wzmianki o karalności takich czynów jak tworzenie i rozpowszechnianie złośliwego oprogramowania (Ventre, 2012).

Pierwsze nieśmiałe kroki w budowaniu instytucjonalno-prawnego zaplecza dla cyberbezpieczeństwa Japończycy podjęli w 1996 r., tworząc Zespół ds. Naruszeń Bezpieczeństwa w Sieci, jednak dopiero po czterech latach pojawiły się pierwsze akty prawne w rodzaju Information Technology Basic Law czy e-Japan Strategy of 2001 (BSA. The Software Alliance [BSA], 2015). Ograniczoną uwagą obdarzono również problematykę infrastruktury krytycznej, wydając okresowo aktualizowany plan akcji Critical Information Infrastrusture, chociaż brakowało agencji mogących podjąć określone kroki

na podstawie obowiązujących wytycznych. Pod tym względem przełomowy okazał się dopiero 2005 r., kiedy powołano do życia Narodowe Centrum Bezpieczeństwa Informacji (NISC). Jako biuro bezpośrednio podlegające premierowi, NISC urosło do rangi centrali cyberdefensywy oraz kluczowej instancji w nadzorowaniu coraz szybciej ewoluującego środowiska internetowego poprzez kompetencje odnoszące się zarówno do sfery prawnej, jak i technicznej. Zatrudnionym w nim urzędnikom powierzono nie tylko uprawnienia legislacyjne, ale też upoważniono do pełnienia funkcji łączników rządu z sektorem prywatnym, zbierania i przetwarzania raportów o działaniach zaczepnych oraz reprezentowania kraju w kontaktach z zagranicą (Matsubara, 2012). Nadane przywileje dalej wynikały z przyjętych przez Narodową Radę Bezpieczeństwa Informacji dokumentów: *First National Strategy on Information Security* (2006) i *Second National Strategy on Information* (2009), czyli pierwowzorów narodowej strategii walki z cyberprzestępczością.

Niemniej aż do 2009 r., gdy przez Azję Wschodnią przetoczyła się fala ataków na organizacje rządowe, media i sektor finansowy, polityka prewencji i zapobiegania pozostawała w znacznym rozproszeniu decyzyjnym pomiędzy odpowiedzialnymi za jej koordynowanie ośrodkami (Tsuchiya, 2011b). Dopiero wydarzenia w sąsiedniej Korei Południowej wpłynęły na bardziej stanowczą reakcję polityków. W latach 2010–2011 Ministerstwo Obrony opublikowało kolejne Białe Księgi obronności, gdzie po raz pierwszy w tak szerokim ujęciu skomentowano zagrożenia wynikające z przekształcenia Internetu w nowoczesną broń. Zwrócono przy tym uwagę na międzynarodowy aspekt problemu, cytując amerykańskie rozwiązania instytucjonalno-prawne w charakterze możliwych do zaadaptowania i godnych naśladowania (m.in. potrzeba utworzenia odpowiednika Cyberdowództwa Stanów Zjednoczonych) (Kallender, 2014). W efekcie wewnątrz ministerstwa powstał dodatkowy pion pod postacią Jednostki Cyberbezpieczeństwa (CDU). Dysponując budżetem w wysokości ponad 140 mln dolarów, komórka uzyskała pełną zdolność operacyjną w 2014 r. i jest wykorzystywana przez japońską armię jako główny organ udaremniający ataki na wszystkie systemy ministerialne (Kshetri, 2016). Również NICS przygotował swój najważniejszy jak dotąd dokument, zatytułowany *Information Security Strategy to Protect the Nation*. Jego oś tworzą trzy podstawowe paradygmaty – wzmocnienie środków przeciwdziałania poprzez reformy polityczne, skuteczniejsza polityka informacyjna oraz zmiana postawy z reakcyjnej na proaktywną *(*Tsuchiya, 2011a).

W 2012 r., niejako antycypując publikację długo oczekiwanej Narodowej Strategii Cybebezpieczeństwa, Ministerstwo Obrony przedstawiło nakierowany wyłącznie na tematykę cyberobronności program *Toward Stable and Effective Use of Cyberspace*, w którym streszczono najbardziej prawdopodobne scenariusze ataku cybernetycznego na Japonię, przedłożono stosowne zalecenia w wymiarze politycznym (m.in. partycypacja w kształtowaniu globalnego prawodawstwa, wzmocnienie pozycji Ministerstwa Obrony i Japońskich Sił Samoobrony), a także zwrócono pilną uwagę na konieczność kooperacji z podmiotami prywatnymi oraz sojusznikami na arenie międzynarodowej. Program podlega corocznej aktualizacji przez Komitet Reagowania, który równocześnie pełni funkcję organu wykonawczego (Ministry of Defence Japan, 2012). Bardziej eklektycznym dokumentem jest przyjęty w 2014 r. *Cybersecucurity Basic Act*, który nie ogra-

nicza się jedynie do sfery obronności, ale zawiera szereg opinii i uwag wystosowanych do przedstawicieli biznesu oraz lokalnej administracji na szczeblu prefektur. Jego podstawowe postulaty sprowadzają się do wzmocnienia kooperacji między poszczególnymi agencjami i organami rządowymi, a najważniejsze rozwiązania praktyczne obejmują wzmocnienie kontroli premiera nad NICS oraz utworzenie Strategicznych Siedzib Cyberbezpieczeństwa, których mnoga nazwa nawiązuje do liczby i rangi zaangażowanych w tę inicjatywę podmiotów Zwoływana cyklicznie konferencja umożliwia wielostronny dialog najważniejszych urzędników odpowiedzialnych za całe spektrum japońskiego cyberbezpieczeństwa – ministrów spraw zagranicznych, obrony, gospodarki i spraw wewnętrznych oraz szefa Narodowej Komisji Spraw Publicznych i szefa rządu (Umeda, 2014).

Kiedy w czerwcu 2013 r. zaczęła w końcu obowiązywać Narodowa Strategia Cyberbezpieczeństwa, Narodowa Agencja Policji (NAP) sformowała składający się ze 140 osób oddział do walki z cyberprzestępczością, który posiada mandat do interweniowania zarówno w kraju, jak i poza jego granicami. Tworzących trzon jednostki fachowców rekrutuje się spośród najbardziej zdolnych pracowników sektora prywatnego, a oprócz doskonałej znajomości środowiska sieciowego funkcjonariusze muszą biegle opanować język angielski, chiński bądź koreański, aby móc swobodnie poruszać się w otoczeniu międzynarodowym. Członkowie oddziału pozostają rozproszeni w trzynastu regionalnych centrach kryzysowych, a ich podstawowe zadanie to wymiana informacji z ponad 4 tys. podmiotów zapewniających kluczowe usługi w ramach układów infrastruktury krytycznej (Kallender, 2014). Podobna mobilizacja zasobów nastąpiła w Ministerstwie Spraw Wewnętrznych, gdzie zainwestowano w budowę Centrum Badań nad Cyberbezpieczeństwem, którego rolą jest rozwijanie technologii obronnych w walce z przestępcami oraz podejmowanie kooperacji w obszarze badań z instytucjami znajdującymi się w Europie oraz Stanach Zjednoczonych (Nitta, 2013).

W 2015 r. Strategia została zweryfikowana i od tego momentu w niezmienionym kształcie pozostaje nadrzędnym aktem zawierającym japońską doktrynę odnoszącą się do problematyki cyberbezpieczeństwa. Dokonując przeglądu dokumentu, łatwo zauważyć, że główny akcent położono na zapewnienie wolności obywateli w dostępie do Internetu, niezależnie od koniecznych ruchów podejmowanych w imię obrony interesów jego użytkowników. Komentatorzy często przytaczają ten punkt, nawiązując do największych słabości Strategii, ponieważ uprawnienia inwigilacyjne służb są przez to znacznie mniejsze, niż ma to miejsce np. w USA. Swobodny przepływ informacji, działanie zgodnie z prawem, pełna otwartość, autonomia w równym korzystaniu z zasobów oraz współpraca stawiana wyżej niż autorytarny nadzór władz konstytuują podstawowe zasady, na jakich opiera się japońska polityka cybernetyczna (The Government of Japan [GoP], 2015). Rozwinięte w dalszej części tekstu założenia identyfikują cztery główne sfery wpływu – poprawę środków bezpieczeństwa odnoszących się do społeczeństwa i gospodarki, budowę internetowego środowiska przyjaznego ludziom, przyczynienie się do wzrostu pokoju i stabilności na arenie lokalnej i międzynarodowej oraz nacisk na badania i rozwój. Osobny artykuł poświęcony konieczności promocji tych rozwiązań

wraz z ich implementacją podnosi znaczenie NISC do rangi głównej placówki odpowiedzialnej za wymienione misje (GoP, 2015).

W Japonii funkcjonuje trzypoziomowa struktura reagowania na przypadki cyberataków. Pierwszy poziom obejmuje aktywność służb policyjnych, którym przyznaje się prawo do zatrzymania i przesłuchania osób podejrzanych o postępowanie niezgodne z przepisami. Jeżeli czyn zostaje przyporządkowany do kategorii zagrożeń godzących w bezpieczeństwo narodowe, wtedy organizacją wskazaną do przeciwdziałania są siły zbrojne, czyli Japońskie Siły Samoobrony. Niezależnie od tej wertykalnej konfiguracji istnieje także wywiad. Jego zadaniem jest prewencja i przewidywanie ataków, zanim dojdzie do ich ucieleśnienia (Tsuchiya, 2011b). Działania wymienionych służb nie są od siebie ściśle odseparowane i wzajemnie się przenikają, a nadzorujące ich pracę NAP, Ministerstwo Obrony oraz NISC tworzą system naczyń połączonych. Przykładowo, policjanci dysponują rozsianymi na terytorium całego państwa punktami stałego monitoringiem ruchu w Internecie, z których dane w razie potrzeby udostępniają pozostałym agencjom. Równocześnie określona grupa ekspertów z Ministerstwa Obrony pozostaje na stałe przydzielona do NISC i współpracuje z tamtejszymi kadrami. Kiedy wspólnie zebrane materiały trzeba poddać gruntownej analizie, wtedy następuje zaangażowanie dalszych aktorów, w tym podlegającej Ministerstwu Spraw Wewnętrznych i Ministerstwu Gospodarki, Handlu i Przemysłu jednostce do zadań specjalnych zwanej Cyber Clean Center (Tsuchiya, 2011b).

Na koniec należy wspomnieć o innych instytucjach, które stanowią rodzaj pomniejszych spoiw regulujących system. Drugą po NICS organizacją odpowiedzialną za ochronę, monitoring i analizę informacji jest rządowa Agencja Promocji Informacji i Technologii, współdziałająca w tym wymiarze z nadal aktywnym Zespołem ds. Naruszeń Bezpieczeństwa w Sieci. Jej podstawowe zadania niejako dublują kompetencje NICS w wymiarze promocji japońskiego sektora IT za granicą, a także odgrywania roli pośrednika pomiędzy stroną rządową a podmiotami uczestniczącymi w prężnie rozwijającym się partnerstwie publiczno-prywatnym (BSA, 2015). Jego członkowie, zrzeszeni w ramach Japońskiej Federacji Biznesu znanej pod nazwą Keidanren, powołali w 2014 r. specjalną radę dbającą o interesy przemysłowców w zakresie bezpieczeństwa teleinformatycznego. Ponad 30 przedsiębiorstw z branży transportu, informatyki stosowanej, komunikacji czy finansów zgłosiło swoich kandydatów, którzy opracowali szereg rekomendacji dla rządu, domagając się zwiększenia nakładów inwestycyjnych w omawianej dziedzinie (Kingston, 2016). Przywiązywanie dużej wagi do bezpieczeństwa danych prywatnych użytkowników wpłynęło na utworzenie pod koniec 2012 r. przez ministra gospodarki Grupy Roboczej ds. Danych Osobistych. Podobny zespół został ulokowany przy Ministerstwie Spraw Wewnętrznych, a owocem jego pracy stał się raport *The Research Society* (Kshetri, 2016). Za kuźnię kadr oraz czołowy ośrodek badawczy uchodzi z kolei założony jeszcze w XIX wieku Narodowy Instytut Technologii Informacyjno-Komunikacyjnej, który rozwija unikatowe narzędzia do walki z cyberprzestępcami. Jego najnowszym osiągnięciem jest umożliwiający śledzenie przebiegu ataku w formule 3D w czasie rzeczywistym program Daedalus, pomagający w ten sposób ustalić źródło zaburzeń (Nitta, 2014a).

Współpraca międzynarodowa

Tradycyjne grupy przestępcze, znane w Japonii pod zbiorczym terminem yakuza, coraz chętniej wykorzystują cybernetyczne metody wyłudzeń i prania brudnych pieniędzy w celu powetowania strat, jakie ponoszą w związku z malejącymi wpływami pochodzącymi z hazardu bądź prostytucji. Ich działalność nie jest jednak głównym powodem do niepokoju, kiedy przeanalizuje się dane dotyczące pochodzenia źródeł inwazji. Studia przeprowadzone przez NAP szacują, że ponad 97% ataków na japońskie instytucje zorganizowano z terytorium innych państw (Nitta, 2014a). Nie jest to zaskakujące, biorąc pod uwagę, że cyberprzestępczość nie jest w żadnym stopniu ograniczona przez czynniki geograficzne czy obcą jurysdykcję. Jej międzynarodowemu rozprzestrzenianiu służy ponadto fakt, że im dalej od miejsca uderzenia znajduje się centrala dowodzenia, tym trudniej jest wyśledzić sprawców. Pozostając pod coraz większym naciskiem ze strony szpiegów, hakerów bądź też pospolitych oszustów, władze Japonii nie mogą skupiać się jedynie na rozwijaniu wewnętrznych zdolności przeciwdziałania, lecz powinny szczególną troską obdarzyć współpracę w ramach regionalnych i globalnych porozumień. Z tego tytułu kraj pozostaje sygnatariuszem najważniejszych międzynarodowych traktatów w rodzaju Konwencji przeciwko cyberprzestępczości z Budapesztu z 2001 r., posiada umowy partnerskie z Sojuszem Północnoatlantyckim i Unią Europejską, a także czynnie uczestniczy w posiedzeniach specjalistycznych ciał powołanych na forum Organizacji Narodów Zjednoczonych (Gady, 2015a).

Implementacja *First National Strategy on Information Security* z 2006 r. stała się przyczynkiem do wyrażenia japońskich ambicji i próby zaakcentowania przez kraj jego roli w budowaniu międzynarodowego porządku odnoszącego się do uniwersum cyberprzestrzeni. Władze planowały nie tylko wzmocnić ówcześnie istniejące mechanizmy, ale otwarcie zakładały rozwój i aplikacje *ściśle japońskiego modelu postępowania* w odniesieniu do występujących już zapisów (Information Security Policy Council, 2006). Model ten charakteryzuje wysoka jakość, efektywność oraz szczególny poziom zaufania. Przygotowana w 2009 r. aktualizacja doktryny pogłębiła te zapewnienia, dodając jednocześnie zapis o gotowości przejęcia przez kraj roli lidera w kontekście bezpieczeństwa informacji w Azji (National Information Security Policy Council, 2009). Obie koncepcje wyraźnie wskazywały, że Japonia od początku optowała za silnym sojuszem odnoszącym się do trójkąta obejmującego Stany Zjednoczone, Stowarzyszenie Narodów Azji Południowo-Wschodniej (ASEAN) oraz Unię Europejską (UE). Bardzo charakterystyczne jest natomiast pomijanie Korei Południowej oraz Chińskiej Republiki Ludowej jako potencjalnych podpór regionalnego partnerstwa, chociaż doświadczenie pierwszej z nich mogłoby okazać się szczególnie cenne. W Narodowej Strategii z 2015 r. żadne z tych państw nie zostało nawet wymienione z nazwy, ustępując pola tak marginalnym z punktu widzenia rzeczywistego znaczenia dla Japonii obszarom, jak Ameryka Południowa, Afryka czy Karaiby (GoP, 2015).

Tak obrana strategia wymusza na Japończykach automatyczny zwrot ku Azji Południowo-Wschodniej, gdzie od 2009 r. w ramach dorocznych ASEAN-Japan Informa-

tion Security Meetings umacniana jest współpraca z państwami regionu. Agenda tych spotkań pozostaje zazwyczaj podobna, a rozmowy sprowadzają się zwykle do trzech podstawowych wymiarów – tworzenia bezpiecznego środowiska dla biznesu, budowy świadomości społecznej w korzystaniu z rozwiązań IT oraz konstruowaniu strategii zarządzania informacją przez poszczególne kraje (*National Center of Incident Readiness and Strategy for Cybersecurity* 2015). Uzupełnieniem dialogu pozostają warsztaty robocze, kursy i treningi, które są tematycznie powiązane z panelami konferencyjnymi. W 2014 r. po raz pierwszy zorganizowano również ASEAN-Japan Cybercrime Dialogue zorientowany na skuteczniejsze wdrażanie założeń konwencji budapesztańskiej oraz zwalczanie aktów cyberprzestępczości i kreowanie regionalnej odporności. Inicjatywy polityków są przy tym wspierane przez przedstawicieli biznesu, czego najlepszym przykładem jest podpisana na początku 2017 r. umowa pomiędzy rządami Filipin, Indonezji, Kambodży, Laosu, Mjanmy i Wietnamu a gigantem japońskiego rynku IT, firmą NEC, która zobowiązała się do dostarczenia technologii oraz przeprowadzenia szkoleń z zakresu cyberbezpieczeństwa dla wymienionych sygnatariuszy (Parameswaran, 2017). Inwestycje na terytorium ASEAN, zarówno te symboliczne w ujęciu politycznym, jak i gospodarcze, stanowią logiczny ruch, który pozwala Japonii zyskać silnego sojusznika przeciwko szerzącym się zagrożeniom. To również okazja do nasycenia rozwijających się rynków ASEAN produktami japońskiego pochodzenia i wyrobienia sobie dominującej pozycji w tamtejszym otoczeniu.

Poza granicami Azji Południowo-Wschodniej bezsprzecznie najważniejszym punktem oparcia dla japońskiej polityki cyberbezpieczeństwa pozostają Stany Zjednoczone. Dla obu państw wzmacnianie zdolności defensywnych w tym obszarze stanowi jedynie wycinek szerszych relacji sojuszniczych, które istnieją od momentu podpisania w 1960 r. traktatu o wzajemnej współpracy i bezpieczeństwie. Japończycy pozostają żywotnie zainteresowani amerykańskim wsparciem, czemu sprzyja ich geograficzne położenie. Ośrodek badań Centrum Studiów Strategicznych i Międzynarodowych wyraźnie stwierdził w najnowszym raporcie poświęconym bilateralnym stosunkom, że Chiny, Korea Północna i Rosja są definiowane jako *główni przeciwnicy* strony japońskiej, jednak Tokio nie posiada odpowiednich zasobów, żeby samodzielnie poradzić sobie z pochodzącym z tych państw niebezpieczeństwem (Lewis, 2015). Pierwsza wspólna deklaracja Japonii i USA dotyczącą zachowania pokoju w cyberprzestrzeni została wydana w 2003 r. pod tytułem *United States-Japan Joint Statement on Promoting Global Cyber Security*. Wezwanie miało za zadanie zwrócić uwagę społeczności międzynarodowej na nadchodzące wyzwania i sugerowało szereg rozwiązań (m.in. partnerstwo sektora publicznego z prywatnym, organizacja multilateralnych for dyskusyjnych, tworzenie mechanizmów wczesnego ostrzegania czy wzmocnienie pozycji rządzących w nadzorze nad sektorem IT), jakie powinny zostać zaadaptowane na rzecz przekrojowej walki z cyberprzestępczością (Department of Defense, 2003). Dopiero po ośmiu latach od ogłoszenia apelu rządy w Tokio i Waszyngtonie oficjalnie przyznały priorytet dwustronnym działaniom na rzecz poprawy bezpieczeństwa w sieci, do czego okazją stało się posiedzenie hybrydowego Amerykańsko-Japońskiego Konsultacyjnego Komitetu Bezpieczeństwa w 2011 r.

Rok później premier Yoshihiko Noda i prezydent Barack Obama po raz pierwszy potwierdzili te zobowiązania na najwyższym szczeblu dyplomatycznym (Matsubara, 2012).

Instytucjonalizacja kontaktów nastąpiła w 2013 r., kiedy w Tokio odbyło się pierwsze ze spotkań w ramach Japan-U.S. Cyber Dialogue, pokrywające tematycznie wszystkie wrażliwe odcinki stanowiące szczególny punkt zainteresowania delegacji japońskiej, w tym infrastrukturę krytyczną, bezpieczeństwo narodowe, budowę zdolności obronnych czy podejście międzynarodowe (Nitta, 2014b). W 2015 r. przedstawiciele Ministerstwa Obrony Japonii i Departamentu Obrony USA wydali wspólny komunikat, w którym zobowiązali się do dalszego wzmacniania zdolności obronnych poprzez mechanizm konsultacji oraz wymianę informacji pomiędzy krajowymi ośrodkami odpowiedzialnymi za gromadzenie danych (U.S.-Japan Cyber Defense Policy Working Group, 2015). Poza wymiarem ściśle politycznym warto odnotować, że amerykański Narodowy Instytut Standaryzacji i Technologii od ponad piętnastu lat utrzymuje bliskie relacje z japońskim Ministerstwem Gospodarki, Handlu i Przemysłu, ustalając wspólne priorytety rozwojowe w dziedzinie cyberbezpieczeństwa i dokonując wymiany dokumentacji technicznej. Publikacje Instytutu skierowane do japońskich odbiorców są tłumaczone i wydawane na tamtejszym rynku. Od 2012 r. rozwinęły się także kontakty biznesowe, kiedy Japońska Federacja Biznesu i Amerykańska Izba Handlowa przeprowadziły pierwszą konferencję poruszającą zagadnienia regulacji handlu w Internecie. Oba podmioty w późniejszym czasie wystosowały odpowiednie rekomendacje do władz państwowych, naciskając na wspieranie procesu zacieśniania relacji pomiędzy sferą prywatną i publiczną (Matsubara, 2012).

Pomimo tych obiecujących sygnałów płynących z obu obozów, ciągle nieuregulowana pozostaje kwestia wpisania zagadnienia cyberbezpieczeństwa do traktatu o wzajemnej współpracy i bezpieczeństwie. Oryginalny tekst powstał w czasach, kiedy pojęcie to nie zostało jeszcze rozpoznane przez prawo międzynarodowe, i wymaga jak najszybszego uzupełnienia. Brak formalnego, osobnego układu odnoszącego się do powyższej tematyki powoduje, że niezdefiniowane pozostają takie dziedziny, jak powinności sojusznicze, możliwe do wdrożenia strategie (defensywne, ofensywne, odpierające) czy regulacje dotyczące wspólnych ćwiczeń wojskowych. Brak obopólnej zgody na to, co właściwie oznacza w przypadku przeciwdziałania atakom cybernetycznym termin *użycie siły* i kiedy takie środki mogą zostać zastosowane, skutecznie ogranicza z kolei pole manewru w łączonych operacjach wojskowych, tropieniu przestępców i podejmowaniu adekwatnych kroków natury odwetowej wobec agresorów (Matsubara, 2012). Wpisany poniekąd w japońską konstytucję pacyfizm to kolejny hamulec, ponieważ pośrednio determinuje on, że zaledwie 1% PKB może być przeznaczony na zbrojenia i obronę, co wpływa również na zasoby finansowe sektora cyberbezpieczeństwa[4]. W konsekwencji, podczas gdy Cyberdowództwo Stanów Zjednoczonych posiada ponad 4 tys. wyszkolo-

[4] Budżet Ministerstwa Obrony Japonii dostępny agencjom odpowiedzialnym za zarządzanie sferą IT wynosi około 160 mln dolarów, podczas gdy Amerykanie wydadzą w 2017 r. na analogiczne cele niemal 20 mld dolarów.

nych funkcjonariuszy podzielonych na trzy odrębne sekcje, to japońska CDU z trudem znalazła środki na zatrudnienie mniej niż setki wojskowych (Kshetri, 2016).

W przeciwieństwie do silnie ugruntowanej współpracy ze Stanami Zjednoczonymi oraz progresywnemu rozwojowi partnerstwa z państwami ASEAN, rozczarowywać może brak głębszego dialogu z najbliższymi sąsiadami Japonii – Chinami i Koreą Południową. W przypadku Chin stosunki nadwątlają czynniki natury historycznej, związane ze zbrodniami Japończyków popełnionymi w Chinach lądowych podczas II wojny światowej, bieżące napięcia powstałe wokół przynależności terytorialnej archipelagu wysp Senkaku, a także podejrzenia kierowane oficjalnymi kanałami w stronę Pekinu, sugerujące udział tamtejszych hakerów w naruszaniu bezpieczeństwa japońskiej sieci. Jeszcze w pierwszej dekadzie XXI wieku za tradycyjne zagrożenie uchodziły operacje prowadzone przez wywiad północnokoreański, który traktował penetrację japońskiego Internetu niczym poligon doświadczalny przed próbami włamań do systemów Korei Południowej. Jednak w 2013 r. Ministerstwo Obrony Japonii po raz pierwszy przyznało, że posiada informacje o tajnej jednostce podporządkowanej Chińskiej Armii Ludowo-Wyzwoleńczej, która prowadzi szpiegostwo technologiczne na terytorium Japonii, a rok później Narodowy Instytut Obronności w Tokio opublikował raport plasujący Chin na czele zestawienia państw używających metody APT w celu kradzieży poufnych informacji rządowych (National Institute for Defense Studies, 2014). Potwierdzenia tych przypuszczeń można doszukiwać się m.in. w wydarzeniach z przełomu lat 2010/2011, kiedy wskutek aresztowania chińskich marynarzy przez japońskie służby ochrony wybrzeża doszło w Chinach do protestów i gróźb użycia *hackingu* pod postacią środka odwetowego (Tsuchiya, 2015). Kilka miesięcy później ofiarami mniej lub bardziej spektakularnych ataków typu DDoS padły korporacje MHI, Toshiba, Fujitsu, a także agencje rządowe i NPA.

Po 2006 r. Japonia stara się pozycjonować w roli regionalnego lidera w walce z problemem cyberprzestępczości i wspierana przez Stany Zjednoczone może się pochwalić określonymi sukcesami. W ograniczonym stopniu inicjatywa przyciągnęła nawet Rosjan, z którymi Japończycy rozwijają w ostatnich latach bliższe kontakty gospodarcze ukierunkowane na korzystanie z zasobów tamtejszego gazu czy handel ropą. Cyberbezpieczeństwo to kolejna możliwa płaszczyzna kooperacji, a uzasadnione nadzieje w tym aspekcie rozbudziło przywrócenie w 2017 r. po trzech latach przerwy rozmów dwustronnych w formacie 2+2, związanych z bezpieczeństwem rejonu Azji i Pacyfiku, gdzie obrona IT stanowi nowy kluczowy temat (Kazak, 2017). W przypadku Chin nie widać obecnie żadnych znaków możliwego odprężenia. Porozumienia z pewnością nie ułatwiają zdarzenia obustronnie antagonizujące zarówno najwyższych dygnitarzy państwowych, jak i społeczeństwa. Aż 71% Japończyków uważa, że stosunki bilateralne pomiędzy krajami są złe, z czym zgadza się niemal 80% ankietowanych w Chinach (Kudo, 2016). Pokazuje to, jak daleko od pozytywnych rozstrzygnięć znajduje się proces dochodzenia do wspólnych stanowisk w obszarze kompatybilnej polityki cybernetycznej. W przeciwieństwie do regionu Azji Południowo-Wschodniej, gdzie siłą wspierającą integrację pozostaje ASEAN, Azja Wschodnia nie ma analogicznej organizacji, która mogłaby dodatkowo stymulować państwa w dziedzinie cyberobronności. Korea Połu-

dniowa, jedyny naturalny partner do rozmów, posiada bardziej rozwinięty potencjał przeciwdziałania cyberterrorowi i prowadzi na tym polu raczej osamotnioną politykę. Skupiona na aktywności północnego sąsiada, nie jest szczególnie zainteresowania przeniesieniem uwagi na pozostałych sąsiadów. Pojedynczym forum wspólnego frontu pozostają odbywające się od 2014 r. trójstronne rozmowy pomiędzy Chinami, Japonią i Koreą Południową, które dotyczą przeciwdziałania północnokoreańskim hakerom, co uzasadnia obecność w tym gronie ostatniego z wymienionych członków i jest potwierdzeniem przytoczonej charakterystyki (Yonhap Agency, 2017).

Bariery w przeciwdziałaniu cybeprzestępczości

Największe wyzwania ogniskujące się wokół problematyki bezpieczeństwa sieci dotyczą przezwyciężenia przez Japonię problemów natury wewnętrznej. Na czołowe miejsce wysuwa się wśród nich brak wyspecjalizowanych pracowników sektora IT, którzy powinni stanowić niezbędną bazę zasobów ludzkich w odpowiedzi na nieprzerwanie rosnące wymagania rynku. Analitycy podkreślają, że w kraju brakuje przynajmniej 80 tys. ekspertów, a według rozmaitych projekcji liczba ta wzrośnie do niemal 200 tys. po 2020 r. (Pollmann, 2016). Jednocześnie wśród obecnie zatrudnionych aż 60% kadry wymaga podniesienia dotychczas zdobytych umiejętności (Department of Commerce, 2016a). Wymusza to dzisiaj na Japończykach konieczność kosztownej dla budżetu kooperacji z partnerami zewnętrznymi w przeprowadzaniu specjalistycznych szkoleń bądź przygotowywania raportów i prowadzenia badań. Nie zastąpi to organizacji własnej służby odpowiedzialnej za ochronę systemów państwowych i prywatnych, lecz postęp nie będzie możliwy, jeżeli w Japonii utrzyma się negatywny trend, za jaki z pewnością należy uznać obcięcie o 50% wydatków na badania i rozwój w sektorze IT w ostatnich latach (Kshetri, 2014). Wątpliwości budzą także warunki pracy stwarzane fachowcom, które różnią się od optymalnych rozwiązań praktykowanych w krajach zachodnich. W porównaniu z rynkiem w Stanach Zjednoczonych, gdzie możliwość pracy w domu dostaje ponad 75% specjalistów, w Japonii współczynnik ten prezentuje się zgoła odmiennie – tylko 25% zatrudnionych ma taką swobodę (Matsubara, Kriz, 2016).

Poważną przeszkodę utrudniającą prewencję stanowi również brak świadomości społecznej i szeroko podzielanej wiedzy wśród japońskich obywateli, która wiązałaby się z ryzykiem, jakim obarczone jest nieostrożne korzystanie z zasobów Internetu. Infantylizacja bądź niezrozumienie znaczenia problemu wynika zarówno z czynników natury demograficznej, jak i kulturowej. Kraj od wielu lat zmaga się z problemem starzenia się populacji, która w przeważającej mierze nie jest zaznajomiona z podstawowymi środkami zachowania ostrożności w Internecie, stając się potencjalnym celem oszustów i złośliwego oprogramowania. Jej dalszą nieufność potęgują takie wydarzenia, jak przytoczony już atak na narodowy system emerytalny z 2015 r., który wzbudził raczej negatywne zainteresowanie i zamiast dać do myślenia, jeszcze bardziej odizolował starsze osoby od współczesnych technologii. W kręgach rządowo-biznesowych kultywowany jest ponadto etos jednostki zaradnej, niepopełniającej błędów i potrafiącej w imię interesów

przełożonych lub wyższego dobra rozwiązać każdy napotkany problem. Z tego powodu Japończycy nie są skłonni dzielić się swoimi doświadczeniami ani też przyznawać do tego, że padli ofiarą cybeprzestępczości w obawie przed napiętnowaniem ze strony współpracowników oraz konkurentów.

Za przykład może służyć zachowanie japońskiego rządu i kwestia raportowania międzynarodowym instytucjom o skali zjawiska cyberataków. Wiarygodne źródła oparte na szczegółowych ankietach potwierdzają, że straty miejscowych firm są mniej więcej w połowie tak duże, jak w przypadku przedsiębiorstw w Stanach Zjednoczonych. Zakładając jednak, że współczynnik strat utrzymuje się w tym państwie na podobnym poziomie jak w innych wysokorozwiniętych krajach (Francja, Niemcy, USA), to przekazywane sprawozdania wydają się zaniżone nawet o 60% (CSIS, 2015). Dodatkową barierą w kształtowaniu prawidłowych postaw jest niechętne stanowisko właścicieli średnich i małych przedsiębiorstw, gdzie tradycyjnie nie przywiązuje się dużej uwagi do rzeczonej problematyki. W przypadku aż 34% z nich cyberbezpieczeństwo nie jest uznawane za istotne wyzwanie rozwojowe dla firm (Matsubara, 2017). Przedstawiciele lokalnego biznesu nie interesują się pozyskiwaniem zaawansowanych usług IT chroniących ich miejsca pracy, co jest praktyką zgoła sprzeczną ze standardami wyznawanymi w państwach, gdzie istnieje równie duże ryzyko ataków. Inwestycje japońskich kompanii handlowo-przemysłowych w programy antywirusowe, certyfikowane chmury obliczeniowe czy narzędzia służące do szyfrowania są średnio o 30% niższe niż u ich amerykańskich odpowiedników (Kshetri, 2016). Zaopatrzenie w tego typu rozwiązania nie jest zresztą najłatwiejsze i najtańsze, ponieważ Japonia paradoksalnie nie posiada żadnego znaczącego przedsiębiorstwa zajmującego się produkcją oprogramowania antywirusowego i jest zmuszona korzystać z zagranicznych licencji (Nitta, 2014a).

Podsumowanie

Zainwestowane w minionej dekadzie środki finansowe, przedłożone regulacje prawne oraz rozwijanie międzynarodowej współpracy z podmiotami dzielącymi podobne stanowiska, pozwoliły Japonii znacząco zwiększyć jej zdolności cyberobronne. Odnotowany skok jakościowy jest szczególnie widoczny, kiedy porówna się dzisiejszą architekturę bezpieczeństwa z sytuacją sprzed regionalnych ataków z 2009 r., które co prawda nie dotknęły kraju w sposób bezpośredni, lecz stanowiły dla władz ostatni dzwonek alarmowy przed nadejściem zupełnie nowej epoki w kontekście identyfikacji współczesnych wyzwań dla bezpieczeństwa narodowego. Nie ulega wątpliwości, że decydującym bodźcem prowadzącym do intensyfikacji proaktywnej polityki cybernetycznej okazało się przyznanie Tokio prawa organizacji letnich Igrzysk Olimpijskich i Paraolimpiady w 2020 r. Nieprzypadkowo pierwsza w historii kraju Narodowa Strategia Cyberbezpieczeństwa została opublikowana na kilka miesięcy przed rozstrzygającym głosowaniem członków Międzynarodowego Komitetu Olimpijskiego, chociaż przez wzgląd na brak gwarancji przejścia kandydatury w dokumencie nie wystąpiły jeszcze czytelne nawiązania do samego wydarzenia. W zaktualizowanej dwa lata później wersji zmiana w treści

była już zasadnicza, a cała strategia została niejako podporządkowana osiągnięciu pełnej gotowości operacyjnej właśnie pod kątem przygotowań do imprezy (GoJ, 2015).

Fakt, że w przypadku poprzedniej Olimpiady doszło do niemal 200 mln ataków na obiekty sportowe, centra logistyczne czy przedstawicielstwa medialne, nie pozostawia już Japończykom więcej czasu do stracenia. W marcu 2014 r., z udziałem ponad 150 zaproszonych ekspertów z całego świata, odbyła się symulacja wielopoziomowego ataku na 21 ministerstw i agencji rządowych oraz wybrane ośrodki przemysłowe. Akcja została zaplanowana na podstawie podobnych ćwiczeń, jakie w 2012 r. przeprowadzono w Londynie. W tym samym miesiącu działalność zainaugurowała specjalna grupa operacyjna złożona z ekspertów IT z poszczególnych ministerstw oraz NAP. Jej celem jest stworzenie spisu rekomendacji i wychwycenie obecnie istniejących uchybień w zaporach sieciowych (Information Management, 2015). Niezależnie od postępów dokonanych w procesie implementacji niezbędnych środków zaradczych, jeden sektor, a mianowicie zasoby ludzkie, wciąż znacząco odbiega od optymalnego kształtu. Należy przy tym odnotować, że w Programie Działania IT na 2017 r. Ministerstwo Spraw Wewnętrznych zwróciło uwagę przede wszystkim na niedostateczną liczbę specjalistów. Na apel pozytywnie odpowiedział Narodowy Instytut Technologii Informacyjno-Komunikacyjnej, tworząc Narodowe Centrum Cyberszkoleń. Zajmuje się ono nie tylko kompleksowym treningiem dla 40 najbardziej zdolnych studentów informatyki w kraju, ale też przygotowuje programy pilotażowe dla pracowników rządu i administracji lokalnej oraz koordynuje pakiet ćwiczeń Cyber Colosseo powiązanych z przygotowaniami do Olimpiady (Matsubara, 2017). Do 2023 r. planowane jest też zwiększenie liczby żołnierzy wchodzących w skład CDU do niemal 1000 osób (Gady, 2017).

Poddana presji czasu, okoliczności oraz konstytucyjnych zapisów, które m.in. zakazują państwu wysyłania żołnierzy na operacje zagraniczne czy uniemożliwiają produkcję broni o charakterze ofensywnym, Japonia coraz bardziej zwiększa swoją odporność w dziedzinie IT. Intensywne wysiłki władz oraz wspierający je sektor prywatny pod postacią największych korporacji IT pokroju NEC, Sony czy Hondy, powinny w najbliższych latach przełożyć się na dobrą zmianę nawyków wśród najbardziej sceptycznych i powoli modernizujących się środowisk – średnich i małych przedsiębiorstw oraz użytkowników indywidualnych. Chęć udziału w tej szeroko zakrojonej mobilizacji zgłaszają też partnerzy zagraniczni. Zauważalny jest znaczący wzrost aktywności amerykańskich oraz izraelskich firm teleinformatycznych, spośród których prym wiodą dostarczające narzędzi szkoleniowych w formie kursów online dla ponad czterdziestu miejscowych spółek Security Innovation oraz pełniący usługi platformy analitycznej Cybereason. Płynący z góry sygnał zaczyna powoli docierać coraz niżej, co widać po zachowania konsumentów, wśród których rośnie zainteresowanie programami zarządzającymi bezpieczeństwem informacji, technologią skanowania podatności sieci oraz produktami kodującymi. Ich rynek urósł w skali ostatniego roku o ponad 5% (UK Trade & Investment, 2015). Reasumując, projekt japońskiej polityki cyberbezpieczeństwa dopiero nabiera ostatecznych kształtów, a z oceną podjętych dotąd wysiłków należy zaczekać przynajmniej do 2020 r. Przy odpowiednim stopniu finansowania i kulturze pracy wewnątrz powołanych w tym celu ciał, efekty wdrożonych rozwiązań powinny sprostać

oczekiwaniom. Wciąż pozostają jednak obszary, które należy wypełnić bogatszą treścią. Inwestycje w zasoby ludzkie, kampanie społeczne nakierowane na uświadomienie ludziom potrzeby przywiązywania większej wagi do zagrożeń płynących z sieci oraz próba wzmocnienia dialogu z Chinami i Koreą Południową to trzy elementy, których spełnienie zagwarantuje Japonii dołączenie do grona państw o najbardziej kompleksowej strategii w ramach polityki bezpieczeństwa Internetu i sprzężonych z nim systemów na świecie.

BILBIOGRAFIA

12.6 million cases of personal information leaked in Japan in 2016, survey shows. (2017). Japan Times. Pobrano 10 lipca 2017, z: http://www.japantimes.co.jp/news/2017/02/28/national/crime-legal/12-6-million-personal-info-leak-cases-seen-japan-2016-card-info-targeted/

Braue, D. (2014). *Japan's banking malware surge pushes Australia out of top 10*. Pobrano 10 lipca 2017, z: https://www.cso.com.au/article/552261/japan_banking_malware_surge_pushes_australia_top_10/

BSA. The Software Alliance. (2015). *Asia-Pacific Cybersecurity Dashboard, Country: Japan*. Pobrano 10 lipca 2017, z: http://www.bsa.org/~/media/Files/Policy/Security/CyberSecure/study_apac_cybersecurity_en.pdf

Center for Strategic and International Studies. (2014). *Net Losses: Estimating the Global Cost of Cybercrime: Economic impact of cybercrime II*. Pobrano 10 lipca 2017, z: https://www.mcafee.com/de/resources/reports/rp-economic-impact-cybercrime2.pdf

Deloitte. (2015). *Asia-Pacific Defense Outlook 2016. Defense in Four Romains*. Pobrano 10 lipca 2017, z: https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Public-Sector/gx-ps-ap-defense-outlook-2016-160216.pdf

Department of Commerce. (2016a). *Japan – Safety and Security*. (2016). Pobrano 10 lipca 2017, z: https://www.export.gov/article?id=Japan-Safety-and-Security

Department of Commerce. (2016b). *Mission Statement. Cyber-security Business Development Mission to Japan, South Korea and Taiwan*. Pobrano 10 lipca 2017, z: http://2016.export.gov/trademissions/cyberasia/

Department of Defense. (2003). *Unitted States-Japan Joint Statement on Promoting Globar Cyber Security*, Final Draft. Pobrano 10 lipca 2017, z: http://web.ita.doc.gov/ITI/itiHome.nsf/51a29d31d11b7ebd85256cc600599b80/1596505329eb670285256de2006de302/$FILE/US-Japan%20Joint%20Statement%20on%20Promoting%20Global%20Cyber%20Security.pdf

Gady, F-S. (2015a). *Japan and Europe Step Up Cooperation in Cyberspace*. Pobrano 10 lipca 2017, z: http://thediplomat.com/2015/01/japan-and-europe-step-up-cooperation-in-cyberspace/

Gady, F-S. (2015b). *Japan Hit by Cybeattacks at an Unprecedential Level*. Pobrano 10 lipca 2017, z: http://thediplomat.com/2015/02/japan-hit-by-cyberattacks-at-an-unprecedented-level/

Gady, F-S. (2017). *Japan's Defense Ministry Plans to Boost Number of Cyber Warriors*. Pobrano 10 lipca 2017, z: http://thediplomat.com/2017/07/japans-defense-ministry-plans-to-boost-number-of-cyber-warriors/

Information Security Policy Council. *The First National Strategy on Information Security*. Pobrano 10 lipca 2017, z: https://www.nisc.go.jp/eng/pdf/national_strategy_001_eng.pdf

Japan Holds Cybersecurity Drill. (2014). *Information Management*, May/June.

Japan pension system hacked, 1.25 million cases of personal data leaked. (2015). Reuters. Pobrano 10 lipca 2017, z: http://www.reuters.com/article/us-japan-pensions-attacks-idUSKBN0OH1OP20150601

Joint Statement of the U.S.-Japan Cyber Defense Policy Working Group. (2015). Pobrano 10 lipca 2017, z: http://www.mod.go.jp/j/press/news/2015/05/30a_1.pdf

Kazak, A. (2017). *Russia, Japan to revive '2+2' format talks, discuss Asia-Pacific security*. Pobrano 10 lipca 2017, z: https://www.rbth.com/international/2017/03/20/russia-japan-talks-asia-pacific-security-722806

Kallender, P. (2014). *Japan, The Ministry of Defense and Cyber-Security*. The Rusi Journal, 159 (1).

Kallender, P, Hughes, W. (2017). Japan's Emerging Trajectory as a 'Cyber Power': From Securitization to Militarization of Cyberspace. *The Journal of Stategic Studies*, 2017, 40(1-2).

Kingston, J. (2016). *Japan's cybersecurity upgrade – too Littre, too late?*. Pobrano 10 lipca 2017, z: http://www.japantimes.co.jp/opinion/2016/05/21/commentary/japans-cybersecurity-upgrade-little-late/#.WW9UzVFLe70

Kshetri, N. (2014). Japan's Changing Cybersecurity Landscape, *Computer*, 47(1).

Kshetri, N. (2016). *The Quest to Cyber Superiority: Cybersecurity Regulations, Frameworks and Strategies of Major Economies*. New York: Springer.

Kudo, Y. (2016). *Polls show Sino-Japan public sentiment worses; direct interaction key to improvement*. Pobrano10 lipca 2017, z: http://www.genron-npo.net/en/opinion_polls/archives/5310.html

Lennon, M. (2011*). Japan's Largest Defense Contractor Hit by Cyber Attack*. Pobrano 10 lipca 2017, z: http://www.securityweek.com/japans-largest-defense-contractor-hit-cyber-attack

Lewis, J-A. (2015). *U.S.-Japan Cooperation in Cybersecurity*. Pobrano 10 lipca 2017, z: https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/151105_Lewis_USJapanCyber_Web.pdf

Matsubara, M. (2012). A Long and Winding Road for Cybersecurity Cooperation Between Japan and United States. *Harvard Asia Quaterly*, 14(1-2).

Matsubara, M. (2017). *How Japan Is Aiming to Close the Cybersecurity Skills Gap Before Tokyo 2020*. Pobrano 10 lipca 2017, z: https://researchcenter.paloaltonetworks.com/2017/05/cso-japan-aiming-close-cybersecurity-skills-gap-tokyo-2020/

Matsubara, M, Kriz, D. (2016), *Putting METI Cyberthreat Information Sharing Recommendation Into Action in Japan*. Pobrano 10 lipca 2017, z: https://researchcenter.paloaltonetworks.com/2016/07/cso-putting-the-meti-cyberthreat-information-sharing-recommendation-into-action-in-japan/

Ministry of Defense Japan. (2012). *Toward Stable and Effective Use of Cyberspace*. Pobrano 10 lipca 2017, z: http://www.mod.go.jp/e/d_act/others/pdf/stable_and_effective_use_cyberspace.pdf

Morgan, S. (2015). *Cybersecurity Market Reaches $75 Billion In 2015; Expected To Reach $170 Billion By 2020. Pobrano 10 lipca 2017*, z: https://www.forbes.com/sites/stevemorgan/2015/12/20/cybersecurity%E2%80%8B-%E2%80%8Bmarket-reaches-75-billion-in-2015%E2%80%8B%E2%80%8B-%E2%80%8Bexpected-to-reach-170-billion-by-2020/

National Center of Incident Readiness and Strategy for Cybersecurity. (2015). *ASEAN-Japan Collaboration on Information Security*. Pobrano 10 lipca 2017, z: https://www.nisc.go.jp/eng/fw_top.html

National Information Security Policy Council. (2009). *The Second National Strategy on Information Security*. Pobrano 10 lipca 2017, z: https://www.nisc.go.jp/eng/pdf/national_strategy_002_eng.pdf

National Institute for Defense Studies. (2014). *NIDS China Security Report 2014: Diversification of Roles in the People's Liberation Army and People's Armed Police*. Pobrano 10 lipca 2017, z: http://www.nids.mod.go.jp/publication/chinareport/pdf/china_report_EN_web_2014_A01.pdf

Nippon Telegraph and Telephone. (2015). *Cybersecurity for Busuness Executives. An NTT publication for top management*. Pobrano 10 lipca 2017, z: http://www.ntt.co.jp/topics_e/CfBE/img/Cybersecurity_for_Business_Executives2.pdf

Nitta, Y. (2013). *Japan's approach towards cyber security*. Pobrano 10 lipca 2017, z: http://cybersummit.info/sites/cybersummit.info/files/Japan_edited%20v2.pdf-FINAL.pdf

Nitta, Y. (2014a). National Cyber Secruity Strategy. Are We Making Progress? Japan's Efforts and Challenges, *Georgetown Journal of International Affairs*, 15(1)

Nitta, Y. (2014b). Review of the Japan Cybersecurity Strategy, *ISPSW Strategy Series: Focus on Defense and International Security*, 290.

Operation Dust Storm, hackers target Japanese Critical Infrastructure. 2015. Cyber Defence Magazine. Pobrano 10 lipca 2017, z: http://www.cyberdefensemagazine.com/operation-dust-storm-hackers-target-japanese-critical-infrastructure/

Parameswaran, P. (2017). *Japan-ASEAN Cyber Cooperation in the Spotlight*. Pobrano 10 lipca 2017, z: http://thediplomat.com/2017/02/japan-asean-cyber-cooperation-in-the-spotlight/

Pawlak, P, Barmpaliou, P-N. (2017). Politics of cybersecurity capacity building: conundrum and opportunity. *Journal of Cyber Policy*, 2(1).

Pollmann, M. (2016). *Japan's Achilles Heel: Cybersecurity*. Pobrano 10 lipca 2017, z: http://thediplomat.com/2016/04/japans-achilles-heel-cybersecurity/,

Record 12,8 billion cyberattacks seen in Japan last year. (2014). *Japan Times*. Pobrano 10 lipca 2017, z: http://www.japantimes.co.jp/news/2014/02/11/business/tech/record-12-8-billion-cyberattacks-detected-in-japan-last-year/#.WWywqVFLe73

The Government of Japan. (2015). *Cybersecurity Strategy*. Pobrano 10 lipca 2017, z: https://www.nisc.go.jp/eng/pdf/cs-strategy-en.pdf

Thomas, N. (2009). Cyber Security in East Asia: Governing Anarchy, *Asian Security*, 5(1).

Tsuchiya, M. (2011a). *Cybersecurity in East Asia: Japan and the 2009 Attacks on South Korea and the United States*. W: Kim. J. Anderson (Red.*), Cybersecurity: Public Sector Threats and Responses*. New York: CRC Press.

Tsuchiya, M. (2011b). Cybersecurity Preparedness in Japan: Rise of Threats in East Asia and Chnge of Administration. Paper presented at the annual meeting of the *International Studies Association Annual Conference Global Governance: Political Authority in Transition*.

Tsuchiya, M. (2015). Japan's Response to Cyber Threats in the Surveillance Age, *Seton Hall Journal of Diplomacy and International Relations*, 17(1-2).

UK Trade & Investment.(2015). *Cyber Security: Policies and Opportunities in Japan*. Pobrano 10 lipca 2017, z: http://www.exporttojapan.co.uk/reports/cyber-security-policies-and-opportunities-japan

Umeda, S. (2014). *Japan: Cybersecurity Basic Act Adopted*. Pobrano 10 lipca 2017, z: http://www.loc.gov/law/foreign-news/article/japan-cybersecurity-basic-act-adopted

Ventre, D. (2012). *Cyberspace in Japan's New Defense Strategy*, W: D. Ventre (Red.), *Cyber Conflict: Competing National Perspectives*. London: Wiley.

Wasilewski, J. (2016). Przestępczość w cyberprzestrzeni – zagadnienia definicyjne. *Przegląd bezpieczeństwa wewnętrznego*, t. 15.

World Economic Forum. (2016). *The Global Information Technology Report 2016*: Innovating in the Digital Economy. Pobrano 10 lipca 2017, z: http://www3.weforum.org/docs/GITR2016/WEF_GITR_Full_Report.pdf

Yonhap Agency. (2017). *S. Korea, Japan, China to discuss N. Korea's cyber threats in Tokyo this week*. Pobrano 10 lipca 2017, z: http://english.yonhapnews.co.kr/news/2017/02/09/0200000000AEN20170209010100315.html